

PCT/JP2004/007112

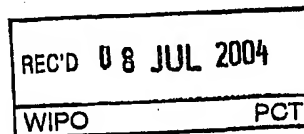
日 本 国 特 許 庁
JAPAN PATENT OFFICE

19.05.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 8 月 2 9 日
Date of Application:



出 願 番 号 特 願 2 0 0 3 - 3 0 7 8 7 2
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 0 7 8 7 2]

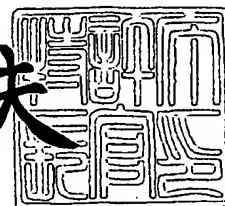
出 願 人 北 川 淑 子
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 6 月 2 1 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 5 5 1 0 8

【書類名】 特許願
【整理番号】 I-MYU-17
【提出日】 平成15年 8月29日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/32
【発明者】
 【住所又は居所】 東京都渋谷区広尾 2丁目3番14号
 【氏名】 北川 高嗣
【特許出願人】
 【識別番号】 500285565
 【氏名又は名称】 北川 淑子
【代理人】
 【識別番号】 100083806
 【弁理士】
 【氏名又は名称】 三好 秀和
 【電話番号】 03-3504-3075
【選任した代理人】
 【識別番号】 100068342
 【弁理士】
 【氏名又は名称】 三好 保男
【選任した代理人】
 【識別番号】 100100712
 【弁理士】
 【氏名又は名称】 岩▲崎▼ 幸邦
【選任した代理人】
 【識別番号】 100087365
 【弁理士】
 【氏名又は名称】 栗原 彰
【選任した代理人】
 【識別番号】 100100929
 【弁理士】
 【氏名又は名称】 川又 澄雄
【選任した代理人】
 【識別番号】 100095500
 【弁理士】
 【氏名又は名称】 伊藤 正和
【選任した代理人】
 【識別番号】 100101247
 【弁理士】
 【氏名又は名称】 高橋 俊一
【選任した代理人】
 【識別番号】 100098327
 【弁理士】
 【氏名又は名称】 高松 俊雄
【手数料の表示】
 【予納台帳番号】 001982
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1

特願 2003-307872

ページ: 2/E

【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0211891

出証特 2004-3055108

【書類名】 特許請求の範囲**【請求項 1】**

認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバにおいて、

前記認証情報を記憶した認証情報記憶装置と、

前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する認証画像生成手段と、

前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を、前記認証端末から取得する認証情報取得手段と、

前記認証パラメータ記憶装置を参照して、前記認証情報取得手段で取得した前記認証画像の情報が、前記認証画像生成手段で生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するか否かを判定し、その結果を前記通信端末に送信する認証情報照合手段

とを備えることを特徴とする情報処理サーバ。

【請求項 2】

前記認証画像生成手段で生成する認証パラメータは、一意に特定できる乱数及び日時 of いずれか一つ以上を含むことを特徴とする請求項 1 に記載の情報処理サーバ。

【請求項 3】

前記認証画像生成手段において、前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、

前記認証情報照合手段において、前記認証情報取得手段によって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする

ことを特徴とする請求項 1 又は 2 に記載の情報処理サーバ。

【請求項 4】

前記認証画像生成手段において、第 1 の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、

前記認証情報取得手段において、前記第 1 の通信ネットワークとは異なる第 2 の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する

ことを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載の情報処理サーバ。

【請求項 5】

前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした情報であることを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の情報処理サーバ。

【請求項 6】

前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の情報処理サーバ。

【請求項 7】

前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求項 1 乃至 6 のいずれか 1 項に記載の情報処理サーバ。

【請求項 8】

前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、

前記認証画像生成手段において、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、

前記認証情報照合手段において、前記結果を前記コンテンツ提供サーバに送信する

ことを特徴とする請求項 1 乃至 7 のいずれか 1 項に記載の情報処理サーバ。

【請求項 9】

認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法において、

前記認証情報を認証情報記憶装置に記憶するステップと、

認証画像生成手段によって、前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する前記認証画像を生成するステップと、

認証情報取得手段によって、前記認証端末から、前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を取得するステップと、

認証情報照合手段によって、前記認証パラメータ記憶装置を参照して、前記認証画像の情報が、前記認証画像を生成するステップで生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するか否かを判定し、その結果を前記通信端末に送信する前記認証情報を照合するステップとを備えることを特徴とする情報処理方法。

【請求項 10】

前記認証画像を生成するステップで生成する認証パラメータは、一意に特定できる乱数及び日時 of the いずれか一つ以上を含むことを特徴とする請求項 9 に記載の情報処理方法。

【請求項 11】

前記認証画像を生成するステップにおいて、前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、

前記認証情報を照合するステップにおいて、前記認証情報を取得するステップによって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする

ことを特徴とする請求項 9 又は 10 に記載の情報処理方法。

【請求項 12】

前記認証画像を生成するステップにおいて、第 1 の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、

前記認証情報を取得するステップにおいて、前記第 1 の通信ネットワークとは異なる第 2 の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する

ことを特徴とする請求項 9 乃至 11 のいずれか 1 項に記載の情報処理方法。

【請求項 13】

前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした情報であることを特徴とする請求項 9 乃至 12 のいずれか 1 項に記載の情報処理方法。

【請求項 14】

前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求項 9 乃至 12 のいずれか 1 項に記載の情報処理方法。

【請求項 15】

前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求項 9 乃至 14 のいずれか 1 項に記載の情報処理方法。

【請求項 16】

前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、

前記認証画像を生成するステップにおいて、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、

前記認証情報を照合するステップにおいて、前記結果を前記コンテンツ提供サーバに送

信する

ことを特徴とする請求項 9 乃至 15 のいずれか 1 項に記載の情報処理方法。

【書類名】明細書

【発明の名称】情報処理サーバ及び情報処理方法

【技術分野】

【0001】

本発明は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理サーバ及び情報処理方法に関する。

【背景技術】

【0002】

現在、インターネットと携帯端末の普及によりいつでもどこでも情報通信を行えるようになってきている。そのため通信される情報が他人に漏れないように様々な暗号化が考えられており、暗号化されたHTTPS (Hypertext Transfer Protocol Security) などのプロトコルを利用して情報をサーバに送信することも頻繁に行われている。

【0003】

携帯端末の場合、規格が通信事業者によって決まるため、例えば、携帯端末を識別する機器識別子を取得することにより、サーバは携帯端末の認証を高い精度で行うことができる。

【0004】

しかし、インターネット等の通信ネットワークにおいて、コンピュータ等の認証を行うことは困難とされている。即ち、コンピュータでインターネット等に接続するために利用するブラウザやHTTP (Hypertext Transfer Protocol) などのプロトコルによれば、携帯端末の様に、コンピュータを識別する識別子を取得しサーバに送信することが不可能である。実際は、ブラウザのクッキーにサーバが作成した暗号化された暗号文を記憶し、認証時にその暗号文をサーバに送信したり、サーバへの接続時にユーザにパスワードを入力させるなどの方法が一般的である。

【0005】

Web上の提携サイトとネットワークを介して接続され、提携サイトへのアクセスが許容されたユーザの認証情報を格納するユーザ情報データベースと、提携サイトへ入力された認証情報を取得し、ユーザ情報データベースに基づいて認証処理を行い、認証結果を提携サイトへ送信する制御手段とを備えた認証システムなどがある (例えば特許文献1)。

【特許文献1】特開2003-6164号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかし上述した特許文献1においては、認証システムにおいてのみ認証されれば、複数の提携サイトについての認証は必要ないが、認証システムにおける認証において盗聴された場合、ユーザの損失は計り知れないものがある。

【0007】

一方、携帯電話機などの携帯端末の普及に伴い、携帯電話を利用して様々なサービスを楽しむユーザが多く、サービスの提供時には氏名、住所などの個人情報を登録する場合がある。この場合、入力するユーザインタフェースに乏しい携帯端末においてこれらの個人情報を登録するのは非常に困難であり、コンピュータでの登録を望むユーザも多い。しかしコンピュータでの登録においては、上述したようなユーザ認証時の問題があり、これを打破するシステムの開発が望まれている。

【0008】

従って本発明の目的は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理サーバ及び情報処理方法を提供することである。

【課題を解決するための手段】

【0009】

上記課題を解決するために、本発明は、認証端末が備える認証情報を利用して、認証情

報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバにおいて、認証情報を記憶した認証情報記憶装置と、通信端末の認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証パラメータ記憶装置に記憶する認証画像生成手段と、通信端末から取得した認証画像の情報と、認証端末が備える認証情報を、認証端末から取得する認証情報取得手段と、認証パラメータ記憶装置を参照して、認証情報取得手段で取得した認証画像の情報が、認証画像生成手段で生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報照合手段とを備える。

【0010】

このような本発明によれば、認証情報を持たない端末でも、認証情報を用いることにより認証を受けることができる。

【0011】

又、認証画像生成手段で生成する認証パラメータは、一意に特定できる乱数及び日時 of いずれか一つ以上を含むことが好ましい。

【0012】

この場合、情報処理サーバで生成した認証パラメータを推測しにくくなるので、より高いセキュリティレベルを保証することができる。

【0013】

又、認証画像生成手段において、認証パラメータ記憶装置に、認証パラメータの有効日時を更に記憶し、認証情報照合手段において、認証情報取得手段によって取得した日時が、認証パラメータ記憶装置に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にすることが好ましい。

【0014】

これによると、認証の有効日時を設けることにより、通信端末と認証端末の間で不正が行われたとしても、その認証を排除することができる。

【0015】

又、認証画像生成手段において、第1の通信ネットワークを利用して通信端末に認証画像を送信し、認証情報取得手段において、第1の通信ネットワークとは異なる第2の通信ネットワークを利用して認証端末から認証画像の情報と認証情報を取得することが好ましい。

【0016】

これによると、別々のネットワークで認証画像と認証情報の送受信を行うので、ネットワークの盗聴が行われても、両方の情報を取得することは非常に困難になる。

【0017】

又、認証画像の情報は、通信端末から取得した認証画像を、認証端末においてデコードした情報であることが好ましい。又、認証画像の情報は、通信端末から取得し、認証端末から受信した認証画像を、デコードした情報であることが好ましい。

【0018】

このような、本発明において送受信される認証情報は、必要な情報が含まれていれば良く、その形態は問わない。

【0019】

又、通信端末から認証画像の情報を取得する場合、認証端末によって、通信端末に提示された認証画像を撮影しデコードすることが好ましい。

【0020】

これによると、認証画像を撮影し、認証端末3でデコードすることにより、ユーザは容易に認証画像を認証端末3に取り込むことができる。又、このデコード時には、認証端末に記憶されたキーを元に復号しても良い。

【0021】

又、情報処理システムは、通信端末にコンテンツを提供するコンテンツ提供サーバを更

に備えており、認証画像生成手段において、コンテンツ提供サーバから、通信端末の認証依頼を受信し、認証情報照合手段において、結果をコンテンツ提供サーバに送信することが好ましい。

【0022】

これによると、情報処理サーバ以外のサーバにおいても、本発明の情報処理サーバの認証機能を用いることにより、高いセキュリティレベルで通信端末を認証することができる。

【0023】

本発明は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法において、認証情報を認証情報記憶装置に記憶するステップと、認証画像生成手段によって、通信端末の認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証パラメータ記憶装置に記憶する認証画像を生成するステップと、認証情報取得手段によって、認証端末から、通信端末から取得した認証画像の情報と、認証端末が備える認証情報を取得するステップと、認証情報照合手段によって、認証パラメータ記憶装置を参照して、認証画像の情報が、認証画像を生成するステップで生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報を照合するステップとを備える。

【0024】

又、認証画像を生成するステップで生成する認証パラメータは、一意に特定できる乱数及び日時 of the いずれか一つ以上を含むことが好ましい。

【0025】

又、認証画像を生成するステップにおいて、認証パラメータ記憶装置に、認証パラメータの有効日時を更に記憶し、認証情報を照合するステップにおいて、認証情報を取得するステップによって取得した日時が、認証パラメータ記憶装置に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にすることが好ましい。

【0026】

又、認証画像を生成するステップにおいて、第1の通信ネットワークを利用して通信端末に認証画像を送信し、認証情報を取得するステップにおいて、第1の通信ネットワークとは異なる第2の通信ネットワークを利用して認証端末から認証画像の情報と認証情報を取得することが好ましい。

【0027】

又、認証画像の情報は、通信端末から取得した認証画像を、認証端末においてデコードした情報であることが好ましい。

【0028】

又、認証画像の情報は、通信端末から取得し、認証端末から受信した認証画像を、デコードした情報であることが好ましい。

【0029】

又、通信端末から認証画像の情報を取得する場合、認証端末によって、通信端末に提示された認証画像を撮影しデコードすることが好ましい。

【0030】

又、情報処理システムは、通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、認証画像を生成するステップにおいて、コンテンツ提供サーバから、通信端末の認証依頼を受信し、認証情報を照合するステップにおいて、結果をコンテンツ提供サーバに送信することが好ましい。

【発明の効果】

【0031】

本発明によれば、認証端末が備える認証情報を利用して、認証情報を備えない通信端末

を認証する情報処理サーバ及び情報処理方法を提供することができる。

【発明を実施するための最良の形態】

【0032】

これによると、

次に、図面を参照して、本発明の実施の形態を説明する。以下の図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。

【0033】

(第1の実施の形態)

図1を参照して、本発明の第1の実施の形態に係る情報処理サーバ1と、情報処理サーバ1を利用した情報処理システムについて説明する。情報処理サーバ1は、中央処理制御装置、メモリなどを備える一般的なコンピュータに所定の処理を実行するソフトウェアプログラムをインストールすることによって実現される。

【0034】

本発明の情報処理サーバ1は、認証端末3が備える認証情報を利用して、認証情報を備えない通信端末2を認証する。ここで、通信端末2は、一般的なコンピュータで、認証端末3は、認証情報を備えた携帯電話機などの通信端末である。認証情報は、指紋認証情報なのでも良いが、本実施の形態においては、情報処理サーバ1が発行した暗号化され改竄不可能な認証識別子であるとする。

【0035】

本発明の実施の形態に係る情報処理システムにおいて、情報処理サーバ1は、第1の通信ネットワーク4aを介して通信端末2と互いに接続可能で、更に、第2の通信ネットワーク4bを介して認証端末3と互いに接続可能である。第1の通信ネットワーク4aと第2の通信ネットワーク4bは、少なくとも一部が互いに交差しない通信ネットワークである。

【0036】

本発明の実施の形態に係る情報処理サーバ1は、認証パラメータ記憶装置101、認証情報記憶装置102、認証識別子記憶装置103、認証画像生成手段111、認証情報取得手段112、認証情報照合手段113、入出力制御手段121を備えている。

【0037】

認証識別子記憶装置103は、情報処理サーバ1が発行した認証端末3を認証するための認証識別子(認証情報)を記憶した記憶装置である。

【0038】

認証画像生成手段111は、通信端末2の認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末2に送信し、認証パラメータを認証パラメータ記憶装置101に記憶する手段である。

【0039】

ここで、認証画像生成手段111で生成し、認証パラメータ記憶装置101に記憶される認証パラメータは、一意に特定できるワンタイムパスワードの様な乱数及び日時 of いくつか一つ以上を含む情報である。この認証パラメータの「日時」は、認証パラメータ生成時の日時でも良いし、通信端末2の認証依頼を受信した日時でも良い。又、認証パラメータ記憶装置101には、認証パラメータを有効にする期限である有効日時も記憶していても良い。認証画像生成手段111は、第1の通信ネットワーク4aを介して通信端末2に認証画像を送信する。ここでは認証画像を送信すると記載したが、認証端末3において情報を解読できれば、テキストでも構わない。テキストの場合、簡単に盗聴できないような桁数の多いものが好ましい。

【0040】

認証情報取得手段112は、通信端末2から取得した認証画像の情報と、認証端末3が備える認証情報を、認証端末3から取得し、認証情報記憶装置102に記憶する手段である。認証情報取得手段112は、第2の通信ネットワーク4bを介して認証端末3から認証情報を受信する。ここで、認証画像の情報は、通信端末2から取得した認証画像を、

証端末3においてデコードした情報であっても良いし、通信端末2から取得し、認証端末3から受信した認証画像を、情報処理サーバ1においてデコードした情報であっても良い。更に、通信端末2から認証画像の情報を取得する場合、認証端末3によって、通信端末2に提示された認証画像を撮影しデコードしても良い。又、通信端末2と認証端末3の間で赤外線通信などの近距離無線通信を利用したり、リムーバブルディスクを利用して、認証端末3は認証画像を取得しても良い。

【0041】

認証情報照合手段113は、認証パラメータ記憶装置101と認証情報記憶装置102と認証識別子記憶装置103を参照して、認証情報取得手段112で取得した認証画像の情報が、認証画像生成手段111で生成された画像の情報であり、更に、認証端末3が備える認証情報が、認証識別子記憶装置103に記憶した認証情報と一致するか否かを判定し、その結果を通信端末2に送信する手段である。更に、認証パラメータ記憶装置101において、認証パラメータの有効日時が記憶されている場合、認証情報取得手段112で取得した日時が、認証パラメータ記憶装置101に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にしても良い。

【0042】

入出力制御手段121は、情報処理サーバ1の入力や出力を制御し、それぞれのネットワークや手段にその情報を伝達する手段である。

【0043】

本発明の実施の形態に係る通信端末2は、認証画像データ記憶装置201、認証画像取得手段211、認証画像提示手段212、認証結果取得手段213を備えている。

認証画像取得手段211は、情報処理サーバ1の認証画像生成手段111によって生成された認証画像を取得し、認証画像データ記憶装置201に記憶する手段である。

認証画像提示手段212は、認証画像データ記憶装置201に記憶された認証画像データを認証端末3に提示する手段である。

更に、認証結果取得手段213は、情報処理サーバ1の認証情報照合手段113によって送信された認証の結果を取得する手段である。

【0044】

本発明の実施の形態に係る認証端末3は、認証画像データ記憶装置301、認証識別子記憶装置302、認証画像撮影手段311、認証情報送信手段312を備えている。

認証画像撮影手段311は、通信端末2の認証画像提示手段212によって提示された画像を撮影し、認証画像データ記憶装置301に記憶する手段である。画像を撮影する必要はなく、通信端末2に送信された認証画像を認証端末3に取得できればどのような手段を用いても構わない。

認証情報送信手段312は、認証識別子記憶装置302に記憶された、情報処理サーバ1から取得した認証識別子と、認証画像データ記憶装置301に記憶された画像の情報を第2の通信ネットワーク4bを介して情報処理サーバ1に送信する手段である。

【0045】

次に、図2を参照して本発明の第1の実施の形態に係る情報処理方法を説明する。

【0046】

まず、ステップS101において情報処理サーバ1は、認証画像生成手段111によって、通信端末2から認証依頼を受信すると、ステップS102において、ワンタイムパスワードや日時などの情報を含む認証画像を生成し、認証パラメータ記憶装置101に記憶する。更にステップS103において、情報処理サーバ1は、生成した認証画像を通信端末2に送信する。

通信端末2は、ステップS103において認証画像を受信すると、受信した画像をステップS104において提示する。

ステップS104において通信端末2で認証画像が提示されると、ステップS105において認証端末3は提示された認証画像を撮影し、認証画像データ記憶装置301に記憶

する。更にステップS106において認証端末3は、認証画像データ記憶装置301に記憶された認証画像の情報と、認証識別子記憶装置302に記憶された認証端末3の認証識別子を併せて認証情報を作成し、ステップS107において、認証情報を情報処理サーバ107に送信する。

【0047】

ステップS107において、情報処理サーバ1は認証端末3から認証情報を受信すると、認証情報取得手段112によって、受信した認証情報を認証情報記憶装置102に記憶し、ステップS108において認証情報照合手段113によって認証パラメータ記憶装置101、認証情報記憶装置102、認証識別子記憶装置103を参照して認証情報の照合を行う。

認証情報の認証結果が出ると、情報処理サーバ1は、通信端末2に認証結果を送信し、通信端末2は認証結果取得手段213によって認証結果を受信する。

【0048】

本発明の第1の実施の形態に係る情報処理サーバ1によると、認証端末3の認証情報を利用することにより、認証情報を備えていない通信端末2を認証することができる。従って、ユーザは一つの認証端末3を備えていれば、複数の端末について同様に認証を受けることができる。

【0049】

更に、本発明の第1の実施の形態によれば、本来は携帯電話機で入力しなければならない情報を、ユーザインタフェースの充実しているコンピュータで入力し、更に、セキュリティレベルの高い状態で、その入力した情報をサーバに送信することができる。

【0050】

(第2の実施の形態)

図3に示した本発明の第2の実施の形態に係る情報処理システムは、図1に示した本発明の第1の実施の形態に係る情報処理システムに比べて、コンテンツ提供サーバ5を備えている点異なる。更に、通信端末2において、認証結果取得手段213を備えておらず、コンテンツ取得手段214を備えている点異なる。

【0051】

本発明の第2の実施の形態に係る情報処理サーバ1は、認証画像生成手段111において、コンテンツ提供サーバ5から、通信端末2の認証依頼を受信し、認証情報照合手段113において、結果をコンテンツ提供サーバ5に送信する。

【0052】

本発明の第2の実施の形態に係るコンテンツ提供サーバ5は、情報処理サーバ1及び認証端末3の情報を利用して通信端末2を認証し、認証された通信端末2にコンテンツを配信するものであって、コンテンツ記憶装置501、認証依頼手段511、認証結果取得手段512、コンテンツ配信手段513を備えている。

コンテンツ記憶装置501は、コンテンツ提供サーバ5が提供するコンテンツが記憶された記憶装置である。

認証依頼手段511は、例えば通信端末2からコンテンツの取得依頼があると、情報処理サーバ1に対して、通信端末2の認証を依頼する手段である。

認証結果取得手段512は、認証依頼手段511で依頼した通信端末2の認証結果を、情報処理サーバ1から取得する手段である。

コンテンツ配信手段513は、通信端末2が認証されると、コンテンツ記憶装置501に記憶されたコンテンツを通信端末2に送信する手段である。

【0053】

図3においては、本発明の第2の実施の形態に係るコンテンツ提供サーバ5は、第1の通信ネットワーク4aに接続されているが、情報処理サーバ1と相互に通信可能ならば、どの通信ネットワークに接続されても良い。

【0054】

図4を参照して、本発明の第2の実施の形態に係る情報処理方法を説明する。

まず、ステップS202において、通信端末2からコンテンツ提供サーバ5にコンテンツの要求がされると、コンテンツ提供サーバ5は、ステップS202において認証依頼手段511によって、情報処理サーバ1に通信端末2の認証を依頼する。

その後、ステップS203乃至ステップ209の処理は、図2のステップS102乃至ステップS108の処理と同様なので説明を割愛する。

【0055】

ステップS209において、情報処理サーバ1において認証結果が出ると、情報処理サーバ1はステップS210において、通信端末2の認証結果をコンテンツ提供サーバ5に送信する。

コンテンツ提供サーバ5は、認証が許可されると、ステップS211においてコンテンツ記憶装置501から通信端末2にコンテンツを提供する。

この方法は、通信端末2において一般的なブラウザを利用してコンテンツ提供サーバ5からコンテンツを取得する場合に有効である。

【0056】

次に、図5を参照して、本発明の第2の実施の形態の変形例に係る情報処理方法について説明する。

まず、ステップS251において、通信端末2がコンテンツ提供サーバ5にコンテンツを要求すると、ステップS252において、コンテンツ提供サーバ5は、通信端末2に認証情報を要求する。

これを受けて通信端末2は、ステップS253において情報処理サーバ1に認証依頼を行う。

その後、ステップS254乃至ステップ260の処理は、図2のステップS102乃至ステップS108の処理と同様なので説明を割愛する。

ステップS260において、情報処理サーバ1において認証結果が出ると、情報処理サーバ1はステップS261において、通信端末2の認証結果を通信端末2に送信し、これを受けて通信端末2は、ステップS262において認証結果をコンテンツ提供サーバ5に送信する。

コンテンツ提供サーバ5は、認証結果を受信すると、認証が許可されている場合、ステップS263においてコンテンツ記憶装置501から通信端末2にコンテンツを提供する。

この方法は、通信端末2ににおいて、コンテンツ提供サーバ5や情報処理サーバ1が提供する認証依頼プログラムを含むアプリケーションによって、コンテンツ提供サーバ5にコンテンツを提供する場合に有効である。

【0057】

本発明の第2の実施の形態によれば、情報処理サーバ1は、複数のサーバの認証機能を受け付けることができ、様々なサーバに高いセキュリティレベルの認証を行わせることができる。

【0058】

(第3の実施の形態)

本発明の第1及び第2の実施の形態においては、通信端末2の認証について主に説明したが、本発明の第3の実施の形態においては、通信端末2及び認証端末3を操作するユーザの認証について説明する。

【0059】

図6に示す本発明の第3の実施の形態に係る情報処理サーバ1は、図1に示す本発明の第1の実施の形態に係る情報処理サーバ1と比べて、リマインダー質疑応答記憶装置104、リマインダー質疑応答登録手段114、パスワード再発行手段115を備えている点異なる。更に、第3の実施の形態に係る認証端末3は、第1の実施の形態に係る認証端末3に比べて、リマインダー質疑応答登録手段313、再発行パスワード取得手段314を備えている点異なる。

【0060】

リマインダー質疑応答登録手段114は、認証端末3のリマインダー質疑応答登録手段313によって複数ある質疑応答のうち、ユーザにユーザが答えられる複数の質疑応答を選択させ、ユーザの認証識別子に関連づけて、そのユーザが選択した質疑応答とその答えをリマインダー質疑応答記憶装置104に記憶する手段である。

【0061】

パスワード再発行手段115は、ユーザがパスワードを忘れてしまった場合、認証端末3の再発行パスワード取得手段314によってパスワードの再発行が要求されると、リマインダー質疑応答記憶装置104を参照してユーザが選択した質問をユーザに答えさせ、リマインダー質疑応答記憶装置104に記憶された応答と一致するかを判定し、全ての質疑に答えられた場合、ユーザにパスワードを発行する手段である。

【0062】

図7に示すように、本発明の第3の実施の形態の情報処理サーバ1が提示する複数の質疑応答は、質疑の候補、応答のセレクトリストの項目を備えている。更に、質疑のジャンルとセレクトリストのセレクト数の項目を備えていても良い。ユーザはこれらの質疑の候補の中から、ユーザ自身が確実に答えられる質問を所定の数（例えば4つなど）以上を、ユーザに選択させる。このようにユーザが登録時に4問以上選択することになる場合、1問から4問以上を選択する組み合わせの数は、1817通りとなる。

【0063】

例えば、「お母さんは何日生まれ？」という質問がユーザに選択されたとすると、セレクトリストとしては1～31日が挙げられ、ユーザはそこから正解を選択する。これらを所定の数だけ繰り返し、認証端末3は、情報処理サーバ1に送信する。例えば、選択数を15の質疑をユーザが4つ選択したとすると、その回答の組合せは、15の4乗となり、50625通りにも及ぶ。このような方法を取ることで、ユーザの選択した質疑とその応答を解読するのは不可能になり、より高いセキュリティレベルを保つことができる。

【0064】

例えば、図8に示すように、英数字だけのパスワードによると、英数字（A～Zまでの英字26文字と0から9までの数字10個）を組合せると、36文字の4乗で1,679,616通りあることを示す。

【0065】

一方、本発明の第3の実施の形態で説明した方法によると、図7に示す様に11の質問から4つを選択し、その4つについて50,625通りのセレクトリストの組合せがあるとする、ユーザがとりうる組合せは、少なく見積もっても91,985,625通り以上となる。これは、図8を参照すると分かるように、英数字のみをパスワードにした場合、5～6桁、数字のみをパスワードにした場合、7～8桁の強度があることが分かる。

【0066】

図9を参照して、本発明の第3の実施の形態に係る情報処理方法について説明する。

まず、リマインダー質疑応答を登録する場合、ステップS301において情報処理サーバ1は認証端末3に質問と、回答の選択肢の組合せを送信し、ユーザに確実に回答できる質問とその答えを決定させる。次に、ステップS302において、情報処理サーバ1は認証端末3から、所定の数以上の質問と回答の組合せを受信し、リマインダー質疑応答記憶装置104に記憶する。

更にパスワードを再発行する場合、ステップS351において、情報処理サーバ1は認証端末3からパスワードの再発行依頼を受信すると、ステップS352において、情報処理サーバ1は認証端末3に、ステップS301で送信した質問と回答の選択肢の組合せと同じものを送信し、ユーザにステップS302で回答した質問に回答させる。

更に、ステップS353において、認証端末3から登録時に回答した質問と回答の組合せを受信すると、ステップS354においてリマインダー質疑応答記憶装置104を参照して回答を照合し、照合の結果、選択した質問と、その質問の回答の全てが一致していた場合、ステップS353においてパスワードを再発行する。

【0067】

本発明の第3の実施の形態に係る情報処理システムによれば、非常に高いセキュリティレベルでユーザを認証することができる。

【0068】

上記のように、本発明の第1乃至第3の実施の形態によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例及び運用技術が明らかとなる。

【0069】

本発明はここでは記載していない様々な実施の形態等を含むことは勿論である。従って、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。

【図面の簡単な説明】

【0070】

【図1】本発明の第1の実施の形態に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

【図2】本発明の第1の実施の形態に係る情報処理方法を示すシーケンス図である。

【図3】本発明の第2の実施の形態に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

【図4】本発明の第2の実施の形態に係る情報処理方法を示すシーケンス図である。

【図5】本発明の第2の実施の形態の変形例に係る情報処理方法を示すシーケンス図である。

【図6】本発明の第3の実施の形態に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

【図7】本発明の第3の実施の形態に係る情報処理サーバがユーザに提示する質問リストとそのセレクトリストの一例である。

【図8】従来のパスワードによる認証の場合の組合せを示した図である。

【図9】本発明の第3の実施の形態に係る情報処理方法を示すシーケンス図である。

【符号の説明】

【0071】

- 1…情報処理サーバ
- 2…通信端末
- 3…認証端末
- 4 a、4 b…通信ネットワーク
- 101…認証パラメータ記憶装置
- 102…認証情報記憶装置
- 103…認証識別子記憶装置
- 104…リマインダー質疑応答記憶装置
- 107…情報処理サーバ
- 111…認証画像生成手段
- 112…認証情報取得手段
- 113…認証情報照合手段
- 114…リマインダー質疑応答登録手段
- 115…パスワード再発行手段
- 121…入出力制御手段
- 201…認証画像データ記憶装置
- 211…認証画像取得手段
- 212…認証画像提示手段
- 213…認証結果取得手段
- 214…コンテンツ取得手段
- 301…認証画像データ記憶装置
- 302…認証識別子記憶装置

- 311...認証画像撮影手段
- 312...認証情報送信手段
- 313...リマインダー質疑応答登録手段
- 314...再発行パスワード取得手段
- 501...コンテンツ記憶装置
- 511...認証依頼手段
- 512...認証結果取得手段
- 513...コンテンツ配信手段

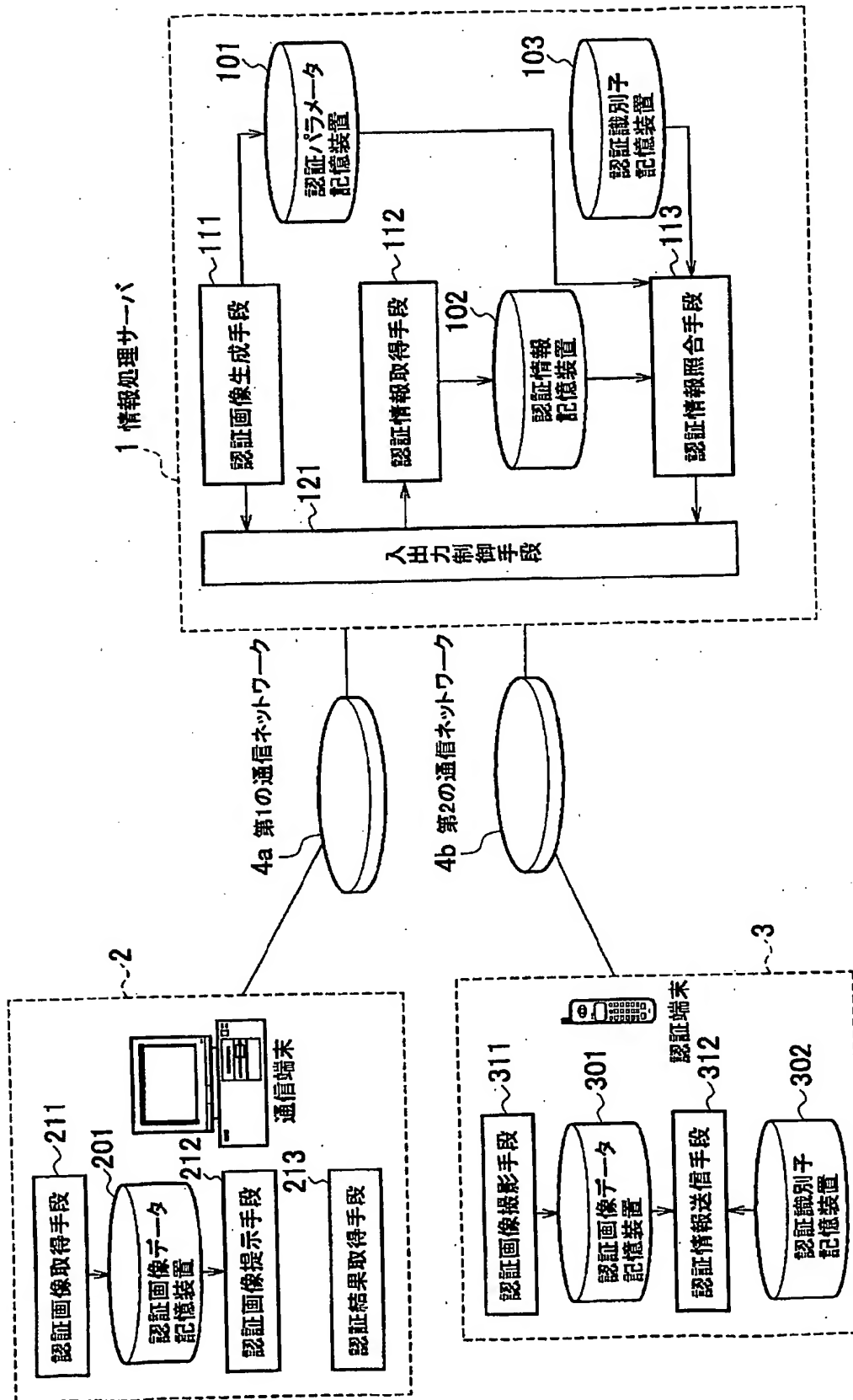
特願 2003-307872

ページ: 1/

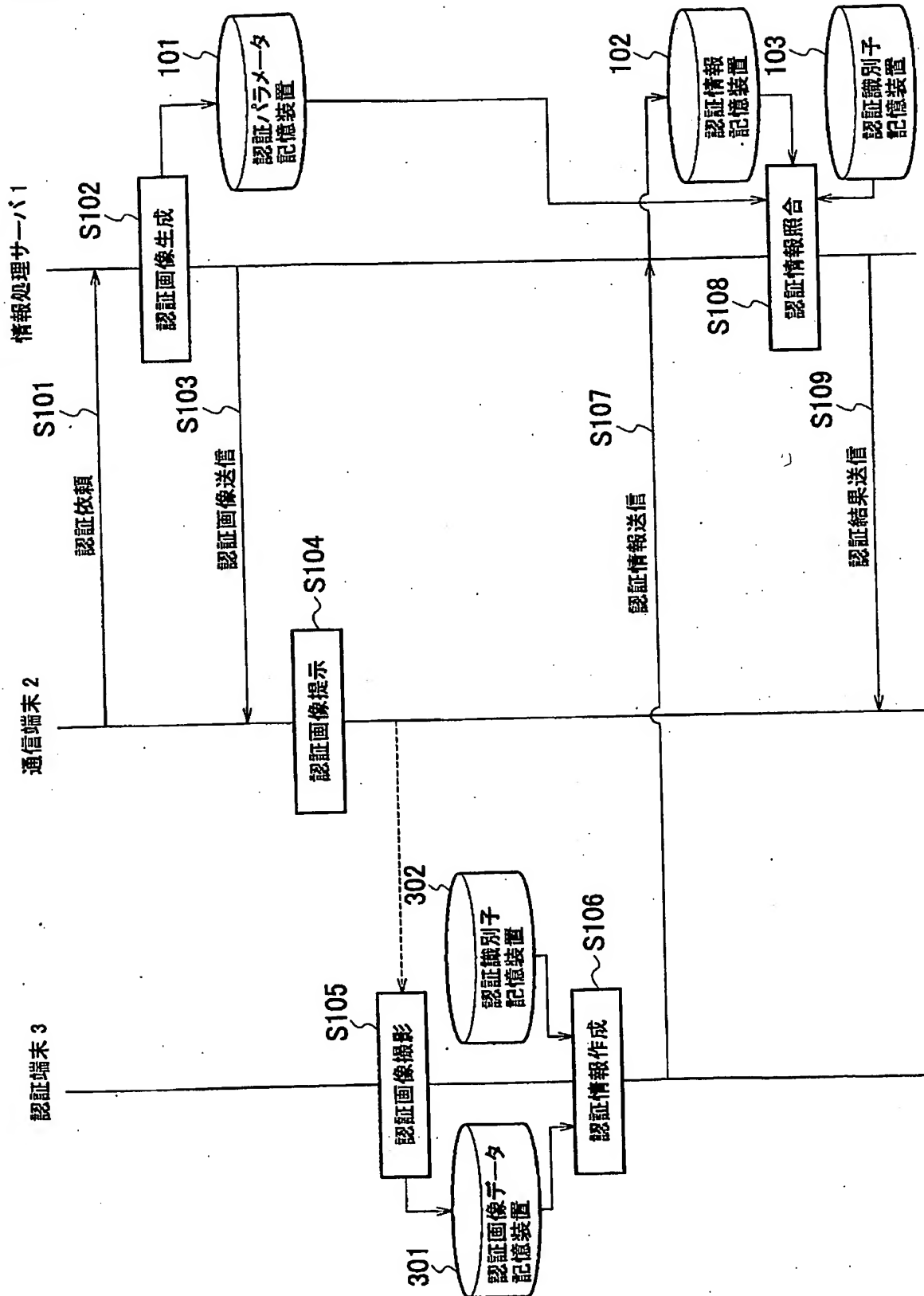
【書類名】 図面

出証特 2004-3055108

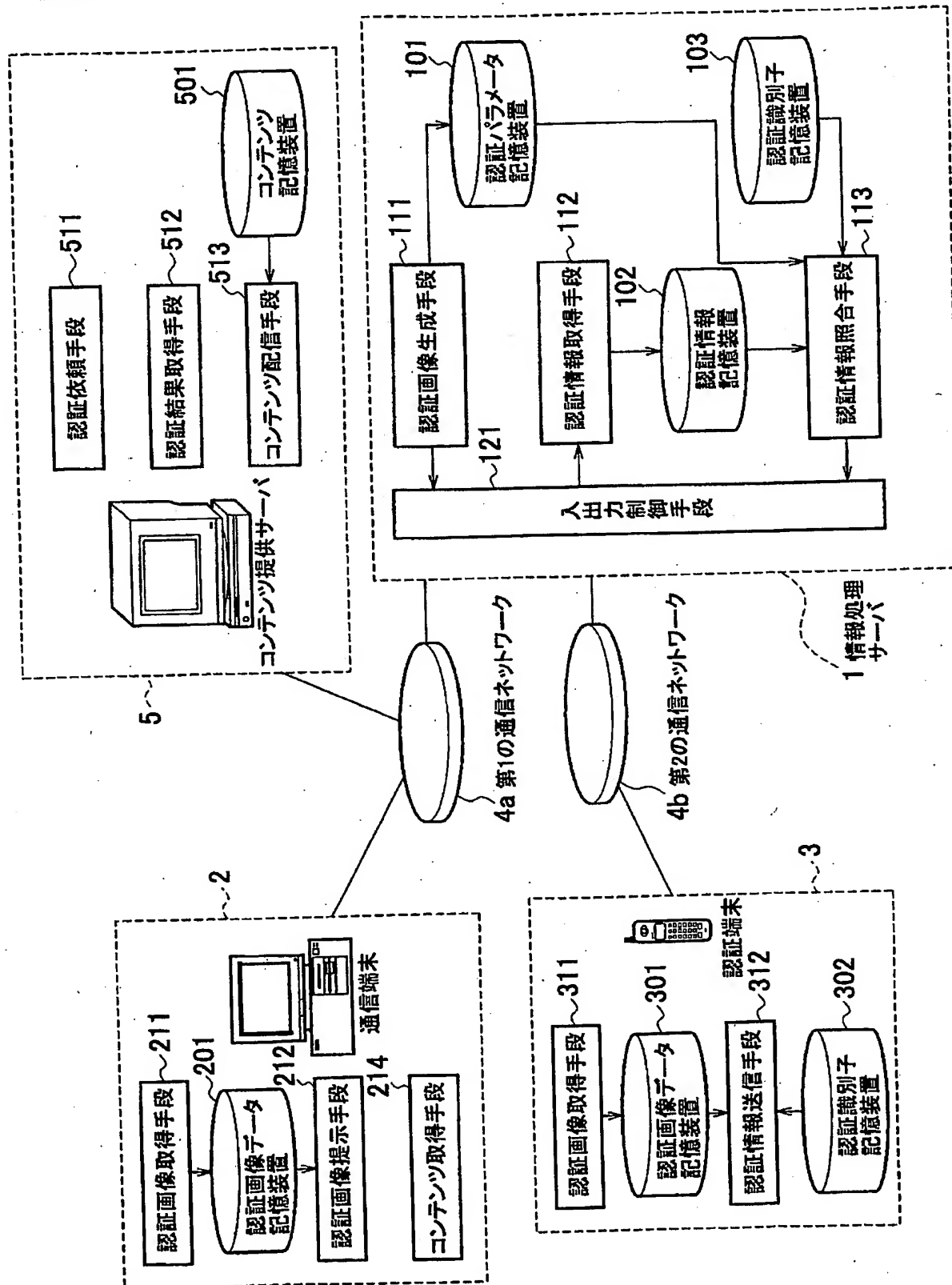
【図1】



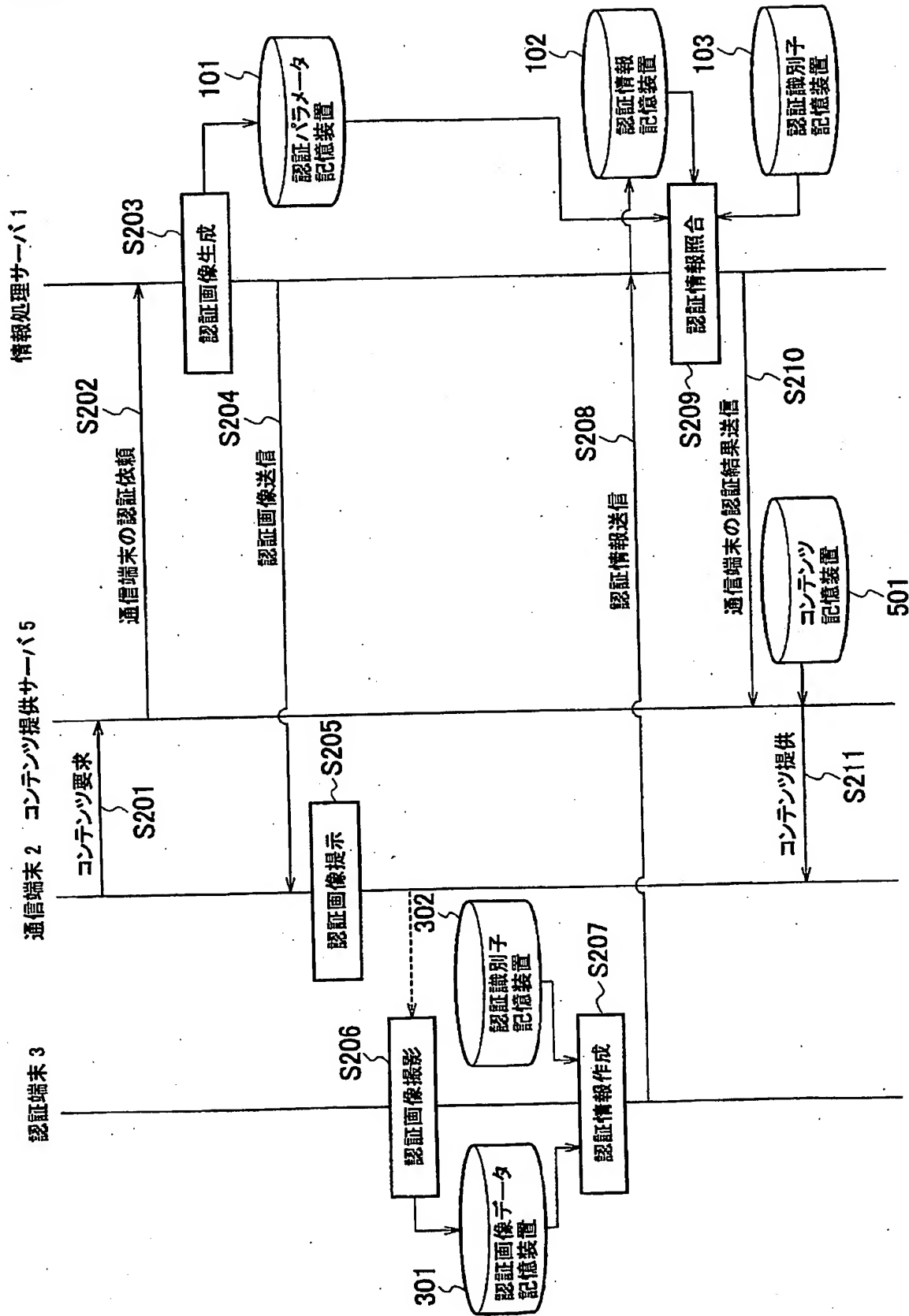
【図2】



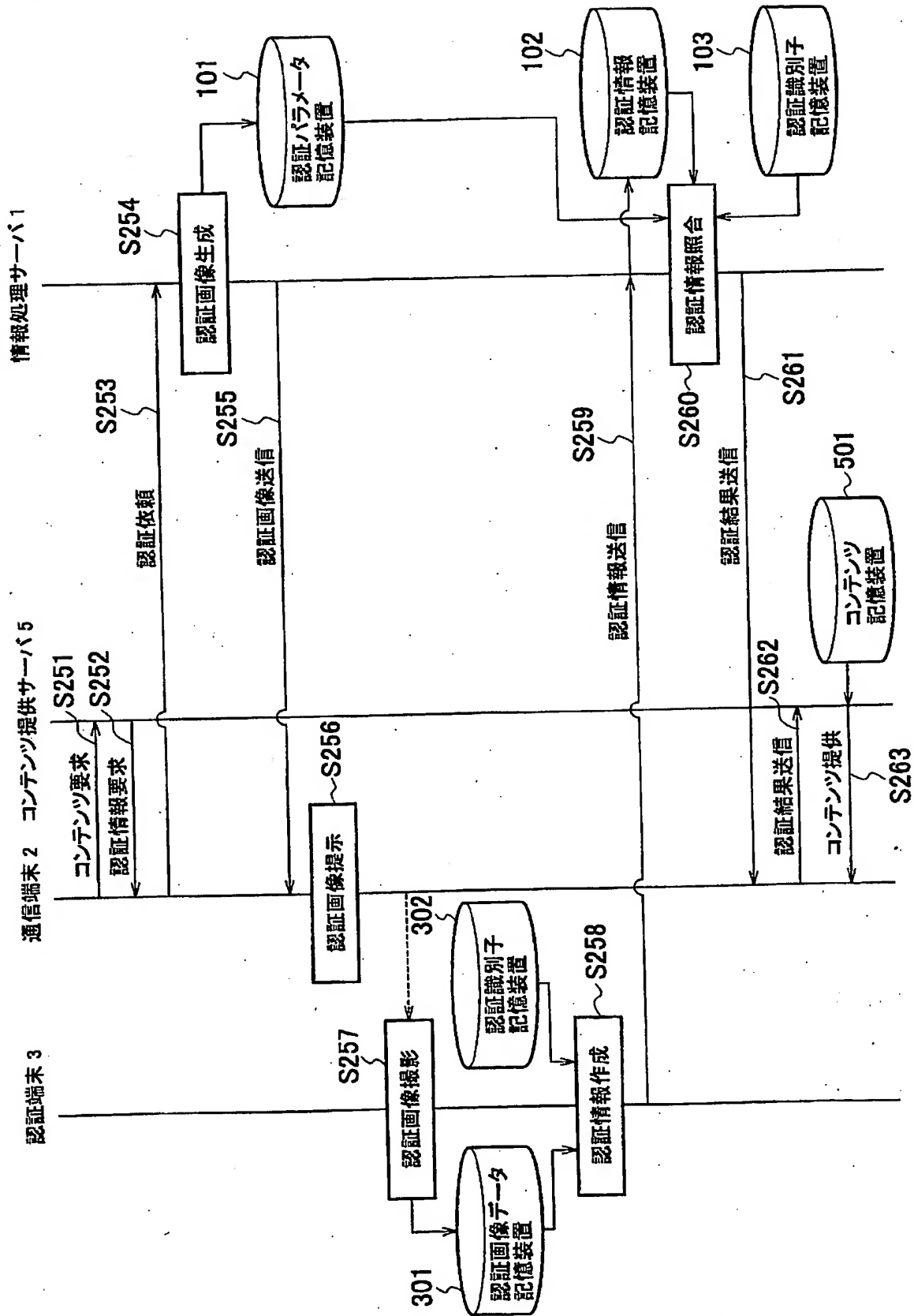
【図3】



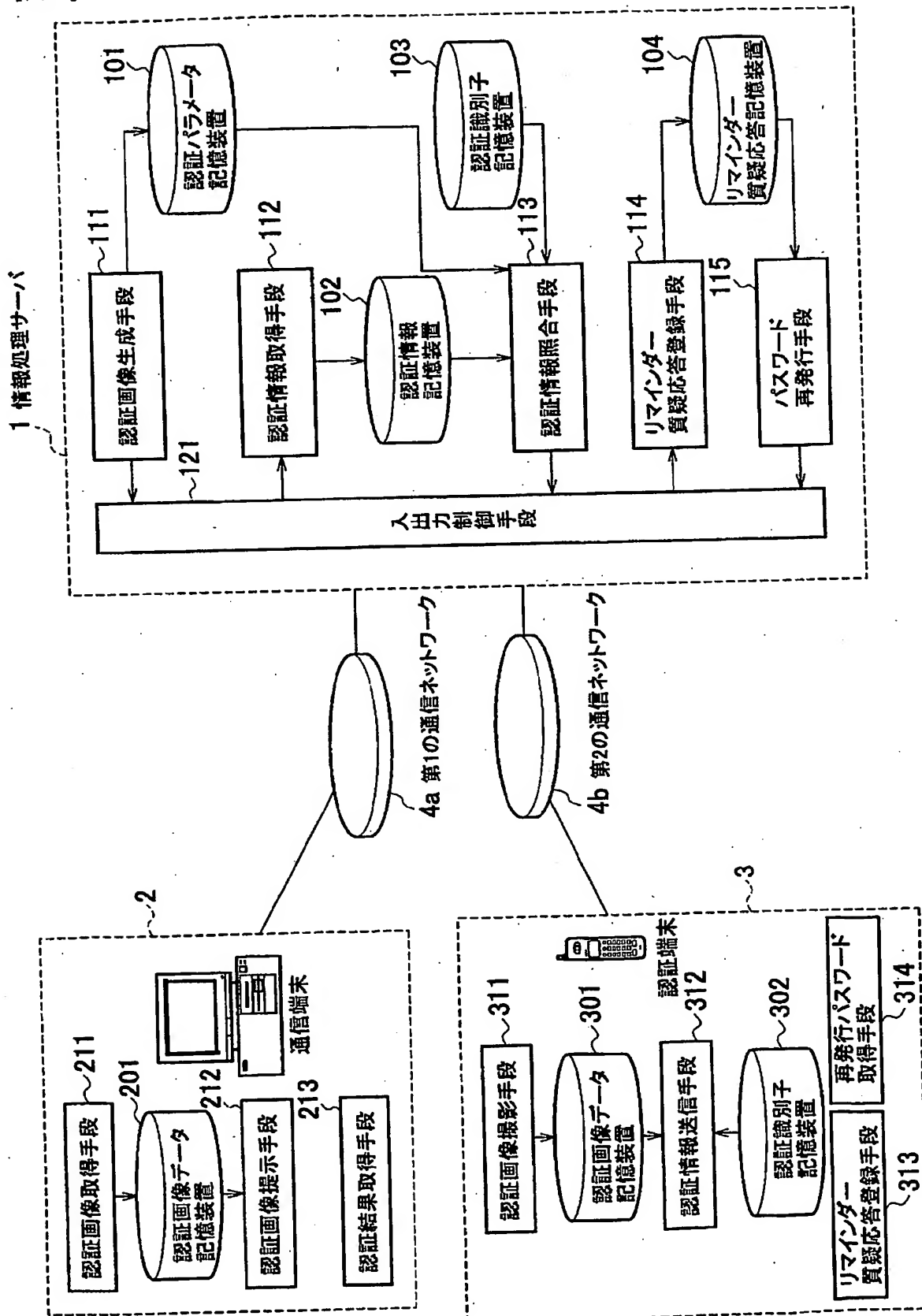
【図 4】



【図 5】



【図6】



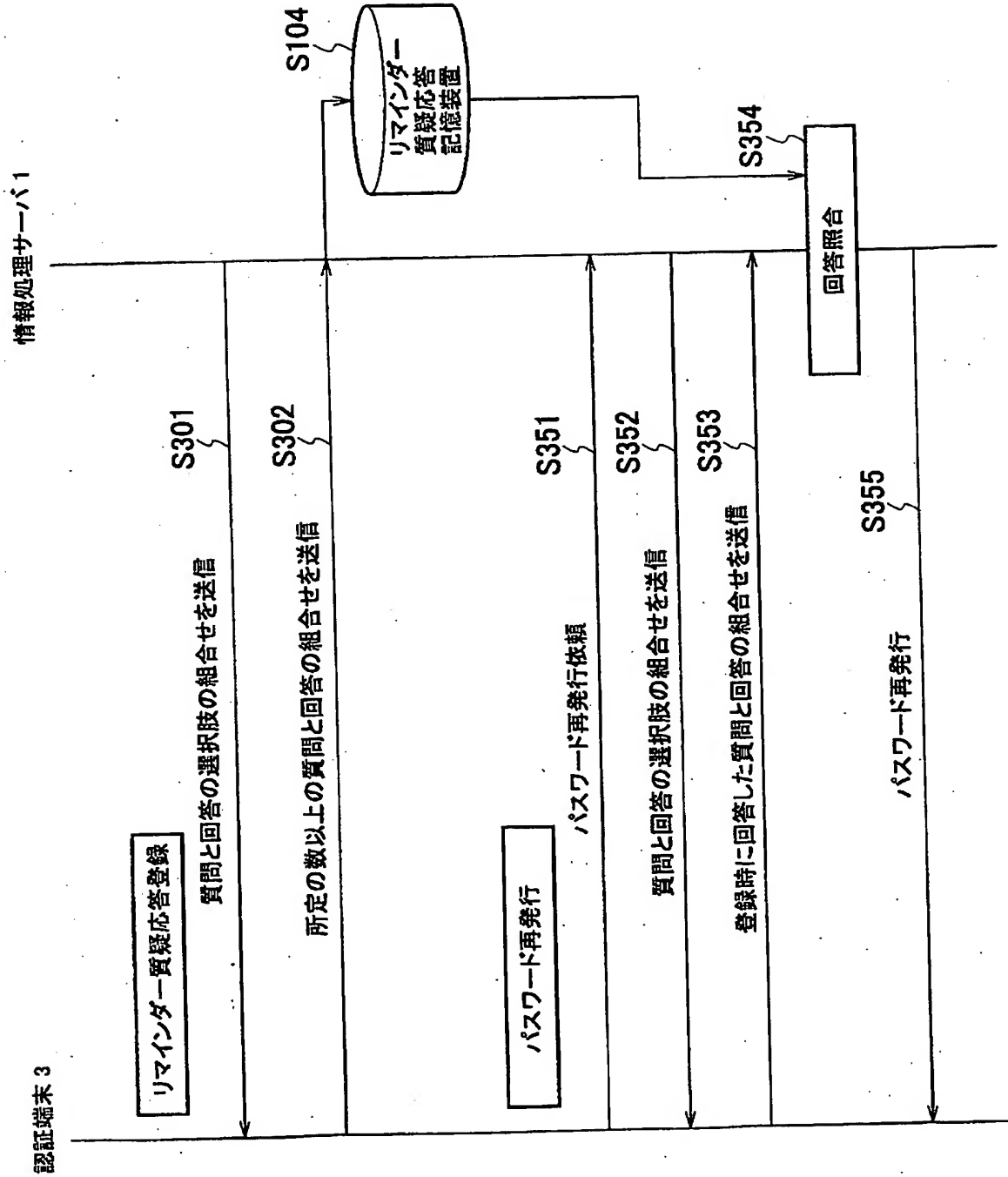
【図 7】

	候補	ジャンル	セレクトリスト	セレクト数
1	お母さんは何日生まれ?	家族	1~31日	31
2	お父さんは何日生まれ?	家族	1~31日	31
3	母親(父親)の旧姓の頭文字は?	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
4	あなたの生まれた市区町村の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
5	初恋の人の苗字の頭文字は?	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
6	最初に飼ったペットの名前の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
7	初めて観た映画のタイトルの頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
8	尊敬する人の苗字の頭文字は?	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
9	母方の祖父の下の名前の頭文字は?	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
10	いとは何人いる?	家族	0~14, 15以上	16
11	初めての担任の先生の苗字の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15

【図 8】

英:A-Z、数:0-9	
4桁(英数)	1,679,616
5桁(英数)	60,466,176
6桁(英数)	2,176,782,336
7桁(英数)	78,364,164,096
8桁(英数)	2,821,109,907,456
4桁(数)	10,000
5桁(数)	100,000
6桁(数)	1,000,000
7桁(数)	10,000,000
8桁(数)	100,000,000

【図 9】



【書類名】要約書

【要約】

【課題】 認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理サーバを提供する。

【解決手段】 情報処理サーバ1は、認証情報を記憶した認証識別子記憶装置103と、通信端末2の認証依頼を受信すると、生成した認証パラメータを含む認証画像を生成して通信端末2に送信し、認証パラメータを認証パラメータ記憶装置101に記憶する認証画像生成手段111と、通信端末2から取得した認証画像の情報と、認証端末3が備える認証情報を、認証端末3から取得する認証情報取得手段112と、認証パラメータ記憶装置101を参照して、認証情報取得手段112で取得した認証画像の情報が、認証画像生成手段111で生成された画像の情報であり、更に、認証端末3が備える認証情報が、認証識別子記憶装置103に記憶した認証情報と一致するか否かを判定し、その結果を通信端末2に送信する認証情報照合手段113とを備える。

【選択図】 図1

特願2003-307872

出願人履歴情報

識別番号

[500285565]

1. 変更年月日

2000年 8月 4日

[変更理由]

住所変更

住所

東京都渋谷区広尾2丁目3番14号

氏名

北川 淑子